(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 24 787 A 1**

(51) Int. Cl.[6]:
H 04 L 9/30
H 04 L 12/22
G 06 F 12/14

(21) Aktenzeichen: 198 24 787.7
(22) Anmeldetag: 3. 6. 98
(43) Offenlegungstag: 16. 12. 99

(71) Anmelder:
Péré, Paul, Dr., 80636 München, DE

(74) Vertreter:
Patentanwälte MÜLLER & HOFFMANN, 81667 München

(72) Erfinder:
gleich Anmelder

(56) Entgegenhaltungen:

US 56 78 041
WO 97 29 428 A1
JP 10-1 11 897 A

TELESEC, Kommunikationssicherheit, Telekom, Produktentwicklung Telesec beim Fernmeldeamt Siegen, 1994, S. 7-14, u. Bild 16-18;
CARAMELLA, D. u.a.: Security management for radiological information systems, In: CAR`97, Computer Assisted Radiology and Surgery, S.1011 (nur Abstract);
PIRET, C.u.a.: Development of a coherent policy of security-confidentiality in a heterogeneous university hospital environment in Belgium, In: Proceedings of Medical Informatics, Europe`96, 1996, S. 951-956 (nur Abstract);

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum abgesicherten Zugriff auf Daten in einem Netzwerk

(57) Durch das erfindungsgemäße Verfahren werden die Datenschutzrechte an insbesondere personenbezogenen Daten gewahrt, die in einem Netzwerk mit verteilten Speichern zur Verfügung stehen. Das Verfahren basiert auf der Vergabe mit Widerrufsmöglichkeit von Inhaber-Zugriffsrechten auf die in dem Netzwerk zur Verfügung stehenden Daten, sowie der Speicherung von Daten innerhalb des Netzwerkes nur nach Autorisierung durch den Inhaber der Rechte an den Daten. Bei einer Anfrage nach bestimmten Daten können nur die Referenzen derjenigen Datensätze angegeben werden, auf die der Anfragende auch die Zugriffsrechte besitzt, wobei vorhandene Daten ohne Zugriffsrechte nicht erkannt werden können. Soll auf bestimmte Daten zugegriffen werden, so kann wiederum eine Überprüfung der Zugriffsrechte erfolgen, bevor ein Datenzugriff erlaubt wird.

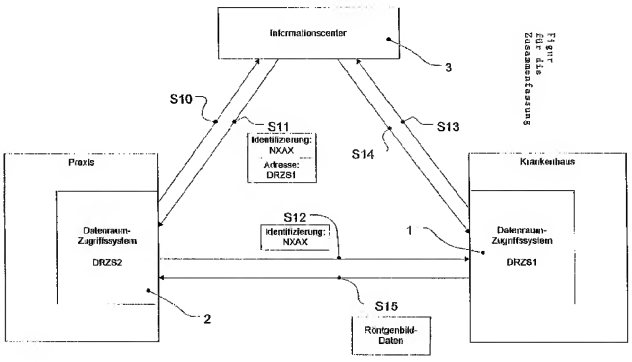


Figure 1 to be published with abstract

DE 198 24 787 A 1

DE 198 24 787 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zum abgesicherten Zugriff auf Daten in einem Netzwerk, im Speziellen in einem Netzwerk mit einem Informationscenter und wenigstens einem Datenraum-Zugriffssystem, wobei unter dem Begriff Datenraum-Zugriffssystem eine Einrichtung verstanden wird, die Speicherplatz (Datenraum) zur Verfügung stellt und den Zugriff auf gespeicherte Daten ermöglicht.

In der nahen Zukunft sollen für unterschiedliche Interessengruppen eines öffentlichen oder privaten Sektors beispielsweise im Gesundheitswesen, etwa für die Krankenkassen, das Gesundheitsministerium und medizinische Zusammenschlüsse, die sogenannten "Praxisnetze" entwickelt werden. Der Grundgedanke dieser Praxisnetze ist es, daß aufgrund einer besseren Kommunikation zwischen unterschiedlichen Arztpraxen und/oder Krankenhäusern zur Zeit häufig noch redundant ausgeführte medizinische Untersuchungen reduziert werden können. In diesem Sinne wäre es z. B. nicht nötig, ein weiteres Röntgenbild einer Lunge eines Patienten zu erstellen, wenn eine erneute Diagnose z. B. eines anderen Arztes unter Zuhilfenahme eines leicht zugänglichen kürzlich aufgenommenen Röntgenbildes der Lunge dieses Patienten möglich wäre. Es liegt im öffentlichen Interesse und dem der Versicherungsgesellschaften, die Gesundheitskosten zu reduzieren, weswegen insbesondere letztere autonome medizinische Netzwerke aufbauen möchten, mit deren Hilfe unterschiedliche Ärzte eines Patienten zu seiner besseren und kostengünstigeren medizinischen Versorgung auch auf die bereits von ihren Kollegen erstellten Daten dieses Patienten zugreifen können.

Bei heute schon aufgebauten Versuchsmodellen besteht das Hauptproblem darin, eine sichere Kommunikation zu gewährleisten. Es sind unterschiedliche Lösungen der Verbindung eines Arztes zu medizinischen Einheiten bekannt, die hauptsächlich auf eine bestimmte Gruppe von Ärzten begrenzt sind, z. B. die Radiologen, wobei naturgemäß eine Beschränkung auf eine spezielle Art der Information/Daten vorgegeben ist, z. B. Röntgenaufnahmen.

Es existieren schon einige nationale und internationale Standards, die die Art der Erzeugung und Übertragung von medizinischen Daten definieren, z. B. DI-COM für Röntgenaufnahmen, BDT für die Daten eines Patienten, GDT für medizinische Daten, die von medizinischen Geräten erzeugt wurden, z. B. von einem Elektrokardiographen oder anderen Einrichtungen. Hierbei werden hinsichtlich der abgesicherten Übertragung von medizinischen Daten keine speziellen Anforderungen gestellt, da dies aufgrund unterschiedlicher bekannter Verschlüsselungsmechanismen heute kein Problem mehr ist.

Eine besondere Aufgabe bei der Übertragung von medizinischen Daten ist es, die individuellen Persönlichkeitsrechte des Patienten zu gewährleisten. Die heute praktizierte Übertragung von medizinischen Informationen ist immer dann illegal, wenn sie nicht auf eine abgeschlossene medizinische Gruppe wie z. B. ein Krankenhaus oder eine Arztpraxis begrenzt ist. Ein Praxisnetz mit hunderten verschiedener Praxen und Krankenhäusern als abgeschlossene Gruppe zu bezeichnen wäre im rechtlichen Sinne wohl als eine Umgehung der Persönlichkeitsrechte von Patienten zu interpretieren. In diesem Fall hätte ein Patient keine Möglichkeit, alle Gruppenmitglieder zu kennen, und könnte von seinem Recht der Auswahl einer anderen Gruppe, wie z. B. eines anderen Krankenhauses, kaum Gebrauch machen.

Demnach liegt der Erfindung die Aufgabe zugrunde, ein Verfahren zum abgesicherten Zugriff auf Daten in einem Netzwerk anzugeben, bei dem nur der Inhaber der Rechte an den Daten frei über diese verfügen kann.

Ein solches Verfahren ist im Patentanspruch 1 angegeben. Vorteilhafte Weiterbildungen dieses Verfahrens finden sich in den Unteransprüchen 2 bis 16.

Nach dem erfindungsgemäßen Verfahren kann allein der Inhaber der Rechte an bestimmten Daten Zugriffsrechte auf diese definieren. Die einmal gespeicherten Daten verbleiben an ihrem Speicherplatz und werden nicht zentralisiert gesammelt. Ein Zugriff auf solche abgespeicherten Daten ist nur mit der Autorisierung des Inhabers der Rechte an diesen Daten möglich. Für medizinische Daten bedeutet dies z. B., daß sie an dem Ort ihrer Erstellung verbleiben und daß andere Ärzte nur mit der Erlaubnis des jeweiligen Patienten auf diese Daten zugreifen können. Eine solche Erlaubnis kann allgemein für bestimmte Ärzte oder auch nur für den Einzelfall erteilt werden. Auch ist es möglich, eine einmal erteilte Erlaubnis wieder zu entziehen.

Die Erfindung und vorteilhafte Weiterbildung werden nachfolgend anhand eines Beispiels unter Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Fig. 1 einen beispielhaften Aufbau eines Netzwerks, in dem das erfindungsgemäße Verfahren Anwendung finden kann;

Fig. 2 die Erzeugung und Abspeicherung von Daten nach dem erfindungsgemäßen Verfahren;

Fig. 3 ein Beispiel einer erfolglosen Anfrage nach bestimmten Daten;

Fig. 4 den Abruf und die Erteilung von Zugriffsrechten an bestimmten Daten durch den Inhaber der Rechte an diesen Daten;

Fig. 5 ein Beispiel einer erfolgreichen Anfrage nach Daten und ihrer Übertragung an die anfragende Stelle.

Im folgenden wird das erfindungsgemäße Verfahren am Beispiel eines Praxisnetzes erläutert. Hier dient das System zur Versorgung einer Gruppe von Ärzten mit den medizinischen Unterlagen ihrer Patienten.

Auf das System können mehrere Ärzte zugreifen, die jeweils einen Zugang auf ein Datenraum-Zugriffssystem haben müssen. Neben diesen Datenraum-Zugriffssystemen weist das System einen Informationscenter auf. In der **Fig.** 1 ist dieses System zur Vereinfachung mit lediglich zwei Datenraum-Zugriffssystemen **1**, **2** gezeigt, von denen eins eine Kennung DRZS1 und das andere eine Kennung DRZS2 aufweist. Solch ein Datenraum-Zugriffssystem **1**, **2** kann am Arbeitsplatz eines oder mehrerer Ärzte aufgebaut sein, z. B. ist in der **Fig.** 1 gezeigt, daß das Datenraum-Zugriffssystem **2** in einer Arztpraxis eines Arztes B und das Datenraum-Zugriffssystem **1** einem Krankenhaus aufgebaut sind, in dem ein Arzt A eine Zugriffsberechtigung dafür besitzt. Jedes Datenraum-Zugriffssystem **1**, **2** kann über ein Netzwerk **4** mit dem Informationscenter **3** oder einem anderen Datenraum-Zugriffssystem **1**, **2** kommunizieren.

Jedes Datenraum-Zugriffssystem **1**, **2** enthält einen sicheren Datenspeicher, in dem die medizinischen Daten von Patienten gespeichert werden können. Dieser Speicher ist dadurch zugriffgesichert, daß ein Datenzugriff nur über das erfindungsgemäße Verfahren erfolgen kann, wodurch ein Datenmißbrauch mit in diesem Speicher gespeicherten Daten nicht möglich ist. Weiter ist durch das erfindungsgemäße Verfahren gewährleistet, daß nur neue Daten gespeichert werden können, also nicht solche, die bereits in einem anderen Datenraum-Zugriffssystem **1**, **2** gespeichert waren. Weiter können sowohl der jeweilige Arzt als auch der Patient unabhängig voneinander über das Datenraum-Zugriffssystem **1**, **2** mit dem Informationscenter **3** oder einem anderen an das Netzwerk **4** angeschlossenen Datenraum-Zugriffssystem **1**, **2** kommunizieren, wobei nur ein Arzt Daten speichern kann.

In dem Informationscenter **3** werden Referenzen zu den

Daten der Patienten und die dazugehörige Identifizierungsinformation der Patienten und Ärzte zentralisiert gespeichert.

Die Sicherheit der einzelnen Datenübertragungen innerhalb dieses Systems wird über eine Verschlüsselung der Datenübertragungen zwischen allen Teilnehmern gewährleistet. Hierbei wird jede innerhalb des Systems übertragene Information mit einer digitalen Signatur versehen. Bei jedem Zugang wird eine Autorisierung verlangt, und alle Daten werden in verschlüsselter Form übertragen und gespeichert. Jeder Teilnehmer, z. B. ein Arzt oder ein Patient, sowie das Informationscenter und jedes Datenraum-Zugriffssystem verfügen über zwei Paare von öffentlichen und geheimen Schlüsseln zur Datenkodierung. Ein Paar dieser Schlüssel, genannt die Verschlüsselungsschlüssel, wird für die sichere Datenübertragung verwendet und das andere, nämlich die Signaturschlüssel, versieht die übertragene Information und bestätigt dadurch den Absender mit einer digitalen Signatur. Die geheimen Schlüssel sind nur dem jeweiligen Teilnehmer, Informationscenter oder Datenraum-Zugriffssystem bekannt, wohingegen die öffentlichen Schlüssel allen Teilnehmern zugänglich sind, d. h., daß jeder in dem System vorhandene Teilnehmer die Möglichkeit hat, einen öffentlichen Schlüssel jedes anderen Teilnehmers zu bekommen. Immer, wenn ein Teilnehmer eine Information über das Netzwerk versendet, wird das folgende Verfahren ausgeführt:

1. Der Sender versieht die von ihm gesendete Information mit einer digitalen Signatur, indem er seinen geheimen Signaturschlüssel verwendet. Hierdurch kann der Sender nicht nachgeahmt werden, wobei der Empfänger eine verwendete digitale Signatur mit Hilfe des öffentlichen Signaturschlüssels bestätigen kann. Wenn z. B. ein Datenraum-Zugriffssystem die Information über einen Patienten an das Informationscenter versendet, muß diese Information bei der Erzeugung von Daten ebenfalls mit dem geheimen Signaturschlüssel dieses Patienten versehen sein. Hierdurch wird gesichert, daß die Information wirklich zu dem benannten Patienten gehört, und daß dieser der Übertragung dieser Information zustimmt.
2. Der Sender verschlüsselt alle übertragenen Daten mittels eines öffentlichen Verschlüsselungsschlüssels des Empfängers, an den die Daten übertragen werden. Hierdurch können diese übertragenen Daten nur unter Verwendung des geheimen Verschlüsselungsschlüssels des Empfängers entschlüsselt werden.
3. Immer, wenn ein Teilnehmer auf das System zugreift, muß er autorisiert sein und seine Identität bestätigt haben. Ein spezieller Datenträger, wie z. B. eine Chipkarte, kann zur Überprüfung der Identität des Teilnehmers dienen. Natürlich können auch andere Verfahren zur Personenidentifizierung eingesetzt werden, wie z. B. die Spracherkennung, die Bilderkennung, die Erkennung von Fingerabdrücken etc., von denen jedes einzeln oder in Kombination eingesetzt werden kann.

Als sicherer Speicher für die geheimen Schlüssel eines Teilnehmers und andere persönliche Information kann ebenfalls ein spezieller Datenträger, wie z. B. eine Chipkarte, eingesetzt werden.

Die öffentlichen Schlüssel der Teilnehmer, des Informationscenter **3** und der einzelnen Datenraum-Zugriffssysteme **1**, **2** können z. B. zentral in dem Informationscenter **3** gespeichert sein.

Die **Fig.** 2 zeigt die Erzeugung von Daten eines Patienten und den Vorgang, wie diese Daten im System zur Verfügung gestellt werden.

Z. B. sucht der Patient N an einem Tag X den Arzt A auf und läßt eine neue medizinische Dateneinheit, z. B. ein Röntgenbild, erstellen. Wenn es der Patient N wünscht, kann diese Dateneinheit über das Praxisnetz anderen Ärzten zur Verfügung gestellt werden. In diesem Fall werden die zu speichernden Daten des Röntgenbildes in einem ersten Schritt S1 in einer elektronischen Form zusammen mit einem elektronischen Formular, welches den Typ der Daten enthält, in dem Datenraum-Zugriffssystem **1** mit der Kennung DRZS1 des Arztes A gespeichert. Der Typ der Daten besteht hier in der Angabe, daß es sich um ein Röntgenbild des Patienten N handelt, das der Arzt A am Tag X aufgenommen hat. Es ist auch möglich, daß der Typ der Daten lediglich aus einer dieser Angaben besteht, oder daß noch weitere Angaben hinzugefügt werden, wie z. B. die Kennung DRZS1 des die Daten speichernden Datenraum-Zugriffssystems **1**. Die Daten des Röntgenbildes werden zusammen mit dem elektronischen Formular in dem gesicherten Datenspeicher des Datenraum-Zugriffssystems **1** gespeichert. Das Speichern von Daten ist nur bei einer Autorisierung des Inhabers der Rechte an diesen Daten möglich, hierzu kann z. B. die Chipkarte des Patienten dienen.

In einem zweiten Schritt S2 wird das Informationscenter **3** von dem Datenraum-Zugriffssystem **1** benachrichtigt, daß es neue Daten aufweist, nämlich ein Röntgenbild des Patienten N. Eine solche Benachrichtigung kann entweder unmittelbar nach der Speicherung der neuen Daten oder zu einem bestimmten Zeitpunkt geschehen, z. B. regelmäßig zu einer bestimmten Uhrzeit. Natürlich ist es auch möglich, daß das Informationscenter **3** zu bestimmten Zeitpunkten Anfragen an jedes Datenraum-Zugriffssystem **1**, **2** schickt, ob neue Daten gespeichert wurden.

In einem dritten Schritt S3 registriert das Informationscenter **3** das Vorhandensein des Röntgenbilds des Patienten N vom Tag X mit der Verfügbarkeit im Datenraum-Zugriffssystem **1** und weist diesen Daten eine nur einfach vorhandene Identifizierung zu, z. B. NXAX, wonach diese Identifizierung mit einer benachrichtigenden Bestätigung vom Informationscenter **3** an das Datenraum-Zugriffssystem **1** übertragen wird. Im Datenraum-Zugriffssystem **1** wird die so zugewiesene Identifizierung zur Verwaltung der zugehörigen Daten verwendet, indem diese zu den Daten hinzugefügt wird. Über eine entsprechende Konfiguration kann gewährleistet werden, daß Daten nicht mehrfach im System vorhanden sind. Spätestens mit der Registrierung der Daten durch das Informationscenter **3** erfolgt hier eine Überprüfung der Autorisierung der Datenspeicherung durch den Patienten. Im Falle der Nichtautorisierung werden keinem Teilnehmer Zugriffsrechte auf diese Daten gewährt.

In der **Fig.** 2, wie auch in den nachfolgenden Figuren bedeutet der hohle Pfeil eine Übertragung von Daten in das System, daß heißt die Speicherung neuer Daten in einem Datenraum-Zugriffssystem **1**, **2**, und die normalen Pfeile jeweils eine Kommunikation über das Netzwerk **4**, wie z. B. eine Anfrage oder Benachrichtigungen. Es kann also anhand der **Fig.** 2 erkannt werden, daß in dem beschriebenen System die medizinischen Daten nicht in das Informationscenter **3** kopiert werden, sondern nach ihrer Speicherung immer im Datenraum-Zugriffssystem **1** verbleiben. Das Informationscenter **3** hält nur die Referenzen zu diesen Daten und niemals die Daten selbst. Weiter wird in den Figuren eine Datenübertragung über das Netzwerk **4** mittels neben normalen Pfeilen dargestellten Rechtecken angezeigt, in denen die jeweils übertragenen Daten angegeben sind.

Die **Fig.** 3 zeigt den Versuch eines Datenzugriffs über das Praxisnetz.

An einem Tag Y besucht der Patient N einen Arzt B, der

ein Datenraum-Zugriffssystem **2** mit der Kennung DRZS2 besitzt. Dieser Arzt B benötigt z. B. ein aktuelles Röntgenbild des Patienten N. Deshalb schickt er in einem Schritt S4 von seinem Datenraum-Zugriffssystem **2** eine Anfrage nach Röntgenbildern des Patienten N an das Informationscenter **3**. Das Informationscenter **3** erstellt eine Liste der Referenzen zu allen Röntgenbildern des Patienten N, die zur Zeit im Gesamtsystem vorhanden sind, d. h. in allen angeschlossenen Datenraum-Zugriffssystemen **1**, **2** gespeichert sind und vom Informationscenter **3** registriert wurden. Anschließend überprüft das Informationscenter **3** die Zugriffsrechte an den in dieser Liste aufgeführten Daten hinsichtlich des Arztes B, von dem die Anfrage über Röntgenbilder des Patienten N kam, und überträgt in einem Schritt S5 lediglich die Referenzen der Röntgenbilder des Patienten N, auf die der Arzt B die Zugriffsrechte vom Patienten N, der in diesem Fall der Inhaber der Rechte an seinen Daten ist, erteilt bekommen hat. Da in diesem Fall z. B. von dem Patienten N noch keine Zugriffsrechte für seine Röntgenbilder definiert wurden, ist diese Liste leer. Deshalb sendet das Informationscenter **3** eine Nachricht "Keine Daten gefunden" an das Datenraum-Zugriffssystem **2**. Dieses gibt diese Nachricht an den Arzt B aus.

Demnach kann ohne Zugriffsrechte des Patienten, der der Inhaber der Rechte an den gespeicherten Daten ist, kein Arzt das Vorhandensein der Daten im System erkennen. Eine Durchbrechung dieses für bestimmte Daten, für die im einzelnen Zugriffsrechte definiert wurden, sicheren Systems ist nur möglich, wenn der Patient N z. B. allgemeine Zugriffsrechte auf seine gesamten Daten oder auf bestimmte Daten im voraus an bestimmte Ärzte gegeben hat. Auch in diesem Fall hat aber der Patient selbst bestimmt, wer auf seine Daten zugreifen kann, also wurden auch hier seine Datenschutzrechte gewahrt.

Die **Fig.** 4 stellt die Definition von Zugriffsrechten des Patienten in dem Informationscenter **3** dar.

Der Patient N kann in einem Schritt S6 z. B. über das Datenraum-Zugriffssystem **2** eine Liste aller seiner zur Zeit im Gesamtsystem zur Verfügung stehenden Daten vom Informationscenter **3** abrufen. Alternativ kann er auch nur eine Liste von bestimmten Daten abrufen. In einem Schritt S7 verarbeitet das Informationscenter diese Anfrage und sendet die jeweils geforderte Liste an das Datenraum-Zugriffssystem **2**. Der Patient N kann jetzt Zugriffsrechte an den durch die Liste aufgezeigten Daten definieren. Hat er z. B. eine Liste aller seiner Röntgenbilder angefordert, so kann er definieren, daß der Arzt B und/oder jeder andere Arzt oder eine bestimmte Gruppe von Ärzten auf das am Tag X vom Arzt A gefertigte Röntgenbild mit der Identifizierung NXAX zugreifen kann. Ein solches Zugriffsrecht kann zeitlich begrenzt oder unbegrenzt sein. Das Zugriffsrecht kann auch im voraus für andere in der Zukunft zur Verfügung stehende Daten vergeben werden. Hat der Patient N alle gewünschten Zugriffsrechte definiert, so kann er in einem Schritt S8 über das Datenraum-Zugriffssystem **2** eine Aktualisierung der Zugriffsrechte im Informationscenter **3** bewirken. Das Informationscenter **3** speichert in einem Schritt S9 die Änderungen und sendet eine Bestätigung zurück an das Datenraum-Zugriffssystem **2**.

Diese Zugriffsrechte können alternativ auch zu dem Zeitpunkt vergeben werden, zu dem neue Daten in einem Datenraum-Zugriffssystem **1**, **2** gespeichert werden. Ein Patient oder sonstiger Inhaber von Rechten an in einem Datenraum-Zugriffssystem **1**, **2** gespeicherten Daten kann Zugriffsrechte von jedem beliebigen Datenraum-Zugriffssystem **1**, **2** aus vergeben. Denkbar wäre es z. B., daß solche Datenraum-Zugriffssysteme **1**, **2** neben ihrem Standort in Arztpraxen oder Krankenhäusern auch in Apotheken aufgestellt werden, oder daß auf ein Praxisnetz auch über das Internet zugegriffen werden kann, wodurch jeder internetfähige Computer zu einem Datenraum-Zugriffssystem oder zumindest zu einem Zugriffssystem werden könnte, welches keinen Speicherplatz zur Verfügung stellt. Der Inhaber der Rechte an in einem Datenraum-Zugriffssystem **1**, **2** gespeicherten Daten, hier also der Patient, ist aufgrund seiner Autorisierung und Identifikation die einzige Person, der die Zugriffsrechte vom Informationscenter **3** angezeigt werden und/oder die sie im Informationscenter **3** modifizieren kann.

Die **Fig.** 5 zeigt den für einen erfolgreichen Zugriff auf bestimmte Daten nötigen Ablauf.

Nach der Definition der Zugriffsrechte an den am Tag X vom Arzt A aufgenommenen Röntgenbild des Patienten N mit der Identifizierung NXAX für den Arzt B durch den Patienten N startet der Arzt B in einem Schritt S10 eine erneute Anfrage an das Informationscenter, alle Referenzen zu den Röntgenbildern des Patienten N anzugeben. In einem Schritt S11 stellt das Informationscenter eine Liste der Referenzen aller zur Zeit in allen Datenraum-Zugriffssystemen vorhandenen Röntgenbilder des Patienten N zusammen, überprüft die Zugriffsberechtigungen hinsichtlich des anfragenden Arztes B und wählt lediglich die Röntgenbilder aus, auf die der Arzt B zugreifen darf, um die zugehörigen Referenzen an das Datenraum-Zugriffssystem **2** zu übertragen, von dem aus der Arzt B die Anfrage an das Informationscenter ausgeführt hat. In diesem Fall wird z. B. nur die Identifizierung NXAX des am Tag X vom Arzt A erstellten Röntgenbildes des Patienten N zusammen mit dem Speicherort/der Adresse, hier das Datenraum-Zugriffssystem **1** mit der Kennung DRZS1, an das Datenraum-Zugriffssystem **2** übertragen, welches dem Arzt B diese Information anzeigt. Der Arzt B kann also nur die Referenzen zu Daten sehen, auf die der Patient N dem Arzt B Zugriffsrechte gewährt hat. Die Referenzen können z. B. die Art der Daten, hier Röntgenbild, das Datum der Untersuchung, hier den Tag X, den untersuchenden Arzt, hier den Arzt A, den Speicherort der Daten, hier das Datenraum-Zugriffssystem **1** mit der Kennung DRZS1, oder auch noch weitere Daten enthalten. In einem Schritt S12 wählt der Arzt B das Röntgenbild mit der Identifizierung NXAX aus, woraufhin das Datenraum-Zugriffssystem **2** eine Anfrage des Arztes B über das Röntgenbild mit der Identifizierung NXAX an das Datenraum-Zugriffssystem mit der Kennung DRZS1, hier das Datenraum-Zugriffssystem **1** sendet. In einem Schritt S13 sendet das Datenraum-Zugriffssystem **1** daraufhin eine Anfrage an das Informationscenter **3**, um zu bestätigen, daß der Arzt B die Zugriffsrechte auf das Röntgenbild mit der Identifizierung NXAX besitzt. Das Informationscenter **3** antwortet in einem Schritt S14 mit einer Bestätigung, woraufhin das Datenraum-Zugriffssystem **1** in einem Schritt S15 die Daten des Röntgenbildes mit der Identifizierung NXAX an das Datenraum-Zugriffssystem **2** überträgt. Dieses stellt die empfangenen Daten des Röntgenbildes in akzeptabler Form dar und/oder läßt den Arzt B die Daten zur weiteren Verarbeitung speichern, wobei eine solche Speicherung nicht in dem sicheren Speicher des Datenraum-Zugriffssystems **2**, sondern auf einem anderen Speichermedium erfolgen muß, denn sonst wären die Daten mehrfach im System vorhanden.

Hat eine berechtigte Person die empfangenen Daten einmal für die weitere Verarbeitung gespeichert, so kann sie natürlich immer wieder auf diese gespeicherten Daten zugreifen. Ein Zugriff über das Praxisnetz ist jedoch nur solange möglich, wie es der Inhaber der Rechte an diesen Daten über die Definition der Zugriffsrechte erlaubt.

Da also nach dem erfindungsgemäßen Verfahren ein Speichern von bestimmten Daten nur mit der Zustimmung des Inhabers der Rechte an diesen Daten möglich ist und auch

ein Abrufen solcher Daten nur mit Zustimmung des Inhabers der Rechte an diesen Daten möglich ist, werden die Persönlichkeitsrechte z. B. eines Patienten gewahrt. Das System arbeitet für jeglichen Benutzer vollkommen transparent, wobei der einzelne Benutzer keine Kenntnisse über die Sicherheits- oder Übertragungsverfahren haben muß. Durch die Verschlüsselung der gesendeten Daten können unberechtigte Personen nicht "mithören" und durch die Definition von bestimmten Zugriffsrechten für bestimmte Daten durch den Inhaber der Rechte an ihnen können keine unberechtigten Datenzugriffe geschehen.

Das erfindungsgemäße Verfahren zum abgesicherten Zugriff auf Daten in einem Netzwerk kann natürlich auch auf andere nicht-medizinische Netzwerke angewandt werden, da hier ein System zur Steuerung der Verteilung individueller Daten vorgeschlagen ist. Ein anderer Anwendungsbereich ist z. B. die Verteilung von Personendaten zu ihrer Identifikation, wodurch die Übertragung dieser Daten z. B. zwischen unterschiedlichen Verwaltungsbehörden ohne eine zentralisierte Datenbank der einzelnen Bürger flexibler gestaltet werden kann. Durch das erfindungsgemäße System hat der nur betroffene Bürger selbst und allein die Verfügungsgewalt über seine individuellen Daten.

Patentansprüche

1. Verfahren zum abgesicherten Zugriff auf Daten in einem Netzwerk mit einem Informationscenter (**3**) und wenigstens einem Datenraum-Zugriffssystem (**1**, **2**), **dadurch gekennzeichnet**, daß allein der Inhaber der Rechte an zu speichernden Daten das Speichern dieser Daten in einem ihm hierzu nicht zugänglichen Datenraum-Zugriffssystem (**1**, **2**) erlauben und die Zugriffsrechte Dritter auf diese Daten in einem Informationscenter (**3**) definieren kann.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß eine Autorisierung der Speicherung von Daten und der Definition der Zugriffs rechte Dritter an den Daten über eine Identitätsprüfung des Inhabers der Rechte an den Daten erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß zu speichernde Daten zusammen mit einem elektronischen Formular, welches den Typ der Daten enthält, in dem Datenraum-Zugriffssystem (**1**) gespeichert werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das Informationscenter (**3**) das Vorhandensein von Daten eines bestimmten Typs in einem Datenraum-Zugriffssystem (**1**) registriert, wonach der Inhaber der Rechte an den gespeicherten Daten in dem Informationscenter (**3**) Zugriffsrechte Dritter auf die Daten definieren kann.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß das Informationscenter (**3**) nach einer Anfrage eines anfragenden Datenraum-Zugriffssystem (**2**) nach Daten eines bestimmten Typs eine Liste der vorhandenen Daten dieses bestimmten Typs unter Angabe des diese Daten jeweils speichernden Datenraum-Zugriffssystems (**1**) an das anfragende Datenraum-Zugriffssystem (**2**) überträgt, für die die Zugriffsrechte des anfragenden Datenraum-Zugriffssystem (**2**) zu den im Informationscenter (**3**) für diese Daten definierten Zugriffsrechten korrespondieren.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß von einem Daten speichernden Datenraum-Zugriffssystem (**1**) bei einer Anfrage nach bestimmten Daten eines bestimmten Typs eines anfragenden Datenraum-Zugriffssystems (**2**) eine Überprüfung der Zugriffsrechte durch eine Anfrage an das Informationscenter (**3**) erfolgt, ob das anfragende Datenraum-Zugriffssystem auf die bestimmten Daten eines bestimmten Typs Zugriffsrechte hat, und die bestimmten Daten eines bestimmten Typs von dem diese Daten speichernden Datenraum-Zugriffssystem (**1**) nur an das anfragende Datenraum-Zugriffssystem (**2**) übertragen werden, wenn das diese Daten speichernde Datenraum-Zugriffssystem (**1**) von dem Informationscenter (**3**) eine Bestätigung erhalten hat.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß ein bestimmte Daten eines bestimmten Typs empfangendes Datenraum-Zugriffssystem (**2**) nur direkt nach einem jeweiligen Datenempfang einen Zugriff auf die empfangenen Daten erlaubt.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß von einem bestimmte Daten eines bestimmten Typs selbst speichernden Datenraum-Zugriffssystem (**1**) ein Zugriff auf die bestimmten Daten eines bestimmten Typs nur gewährt wird, wenn eine positive Überprüfung der Zugriffsrechte durch eine Anfrage an das Informationscenter (**3**) erfolgt ist, ob das die bestimmten Daten eines bestimmten Typs selbst speichernde Datenraum-Zugriffssystem (**1**) für die bestimmten Daten eines bestimmten Typs Zugriffsrechte vorweisen kann.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß das Informationscenter (**3**) von einem neue Daten aufweisenden Datenraum-Zugriffssystem (**1**) über das Vorhandensein neuer Daten eines bestimmten Typs benachrichtigt wird, woraufhin das Informationscenter (**3**) eine benachrichtigenden Bestätigung an das betreffende Datenraum-Zugriffssystem (**1**) sendet.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß die Daten anhand einer vom Informationscenter (**3**) zugewiesenen nur einfach vorhandenen Identifizierung identifiziert werden, die von dem Informationscenter (**3**) nach einer Registrierung von neuen Daten an das diese Daten speichernde Datenraum-Zugriffssystem (**1**) übertragen wird, damit dieses die jeweilige Identifizierung an die jeweiligen Daten anhängt.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß das Informationscenter (**3**) nach einer Anfrage über Daten eines bestimmten Typs von einem Datenraum-Zufgriffssystem (**2**) eine Liste aller vorhandenen Daten dieses bestimmten Typs erstellt, bevor es die Zugriffsrechte auf die Daten des bestimmten Typs überprüft, um die Liste der vorhandenen Daten dieses bestimmten Typs unter Angabe des diese Daten jeweils speichernden Datenraum-Zugriffssystems (**1**) an das anfragende Datenraum-Zugriffssystem (**2**) zu übertragen, für die das anfragende Datenraum-Zugriffssystem (**2**) die Zugriffsrechte vorweisen kann.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß bei einem gewünschten Datenzugriff von einem Datenraum-Zugriffssystem (**1**) auf Daten eines bestimmten Typs zunächst eine Anfrage nach solchen Daten des bestimmten Typs an das Informationscenter (**3**) geschickt wird.

13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, daß bei einer gewünschten Datenübertragung von einem Daten speichernden Datenraum-Zugriffssysten (**1**) an ein anfragendes Datenraum-Zugriffssystem (**2**) von diesem zunächst eine An-

frage nach bestimmten Daten eines bestimmten Typs an das diese bestimmten Daten eines bestimmten Typs speichernde Datenraum-Zugriffssystem (**1**) geschickt wird.

14. Verfahren nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, daß die Daten in einem Datenraum-Zugriffssystem (**1**, **2**) in einem sicheren Datenspeicher gespeichert werden, wobei auf die darin gespeicherten Daten kein direkter Zugriff möglich ist.

15. Verfahren nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, daß der Typ der Daten durch ihren Inhalt und/oder den Inhaber der Rechte an den Daten bestimmt wird.

16. Verfahren nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, daß die Zugriffsrechte an gespeicherten Daten durch den Inhaber der Rechte an den Daten zu einem beliebigen Zeitpunkt nach ihrer Registrierung in dem Informationscenter (**3**) definiert werden können und danach durch eine Neudefinition von dem Inhaber der Rechte an den Daten beliebig wieder geändert werden können.

17. Verfahren nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, daß die Zugriffsrechte an gespeicherten Daten durch den Inhaber der Rechte an den Daten mit ihrer Speicherung in einem Datenraum-Zugriffssystem (**1**, **2**) vergeben werden können.

18. Verfahren nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, daß die Kommunikation zwischen einem Datenraum-Zugriffssystem (**1**, **2**) und dem Informationscenter (**3**) oder einem anderen Datenraum-Zugriffssystem (**2**, **1**) verschlüsselt erfolgt.

19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, daß der Sender die von ihm gesendete Information mittels einem geheimen Signaturschlüssels mit einer digitalen Signatur versieht, wodurch der Empfänger die gesendete Information mittels eines dazugehörenden öffentlichen Signaturschlüssels überprüfen kann.

20. Verfahren nach Anspruch 18 oder 19, dadurch gekennzeichnet, daß daß der Sender alle übertragenen Daten mittels eines vom Empfänger ausgegebenen öffentlichen Verschlüsselungsschlüssel kodiert, wodurch nur der Empfänger die übertragenen Daten mittels eines geheimen Verschlüsselungsschlüssels dekodieren kann.

21. Verfahren nach einem der Ansprüche 18 bis 20, dadurch gekennzeichnet, daß sowohl jedes Datenraum-Zugriffssystem (**1**, **2**) und das Informationscenter (**3**) als auch jeder Teilnehmer je einen geheimen und je einen öffentlichen Signaturschlüssel und Verschlüsselungsschlüssel aufweisen.

22. Verfahren nach Anspruch 21, dadurch gekennzeichnet, daß die geheimen Signaturschlüssel und Verschlüsselungsschlüssel und/oder öffentlichen Signaturschlüssel und Verschlüsselungsschlüssel eines Teilnehmers auf einem Datenträger, wie z. B. einer Chipkarte, gespeichert sind.

23. Verfahren nach einem der Ansprüche 1 bis 22, dadurch gekennzeichnet, daß sich ein auf das Netzwerk zugreifender Teilnehmer autorisieren muß und seine Identität vom Informationscenter überprüft wird.

24. Verfahren nach Anspruch 23, dadurch gekennzeichnet, daß die Identität eines Tellnehmers auf einem Datenträger, wie z. B. einer Chipkarte, gespeichert ist.

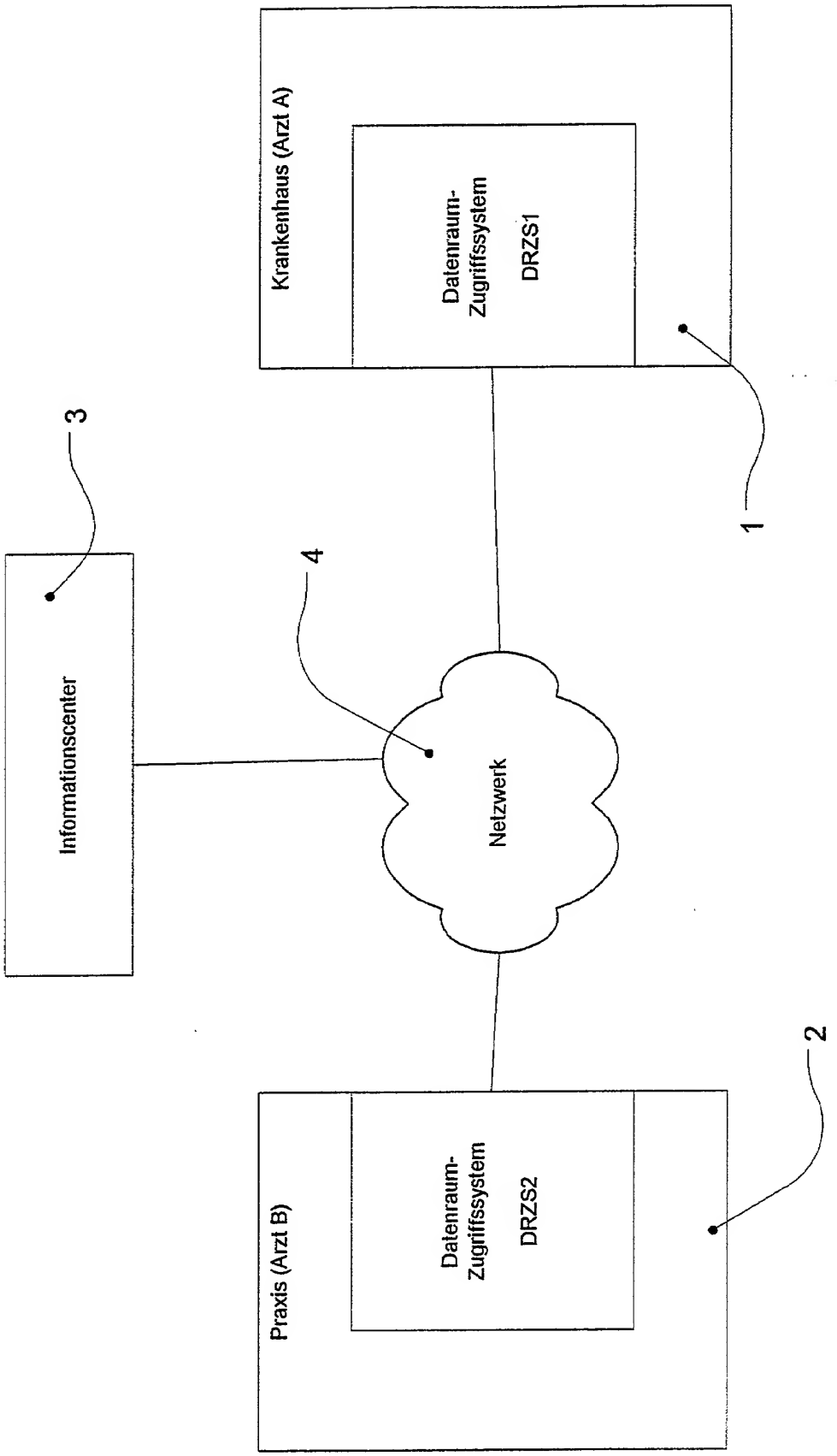
25. Verfahren nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, daß die Erlaubnis der Speicherung der Daten durch den Inhaber der Rechte an den Daten spätestens bei einer Registrierung der Daten in dem Informationscenter (**3**) erfolgt, wobei das Informationscenter (**3**) ohne korrekte Autorisierung keinen späteren Datenzugriff auf diese Daten erlaubt.

Hierzu 5 Seite(n) Zeichnungen

- Leerseite -

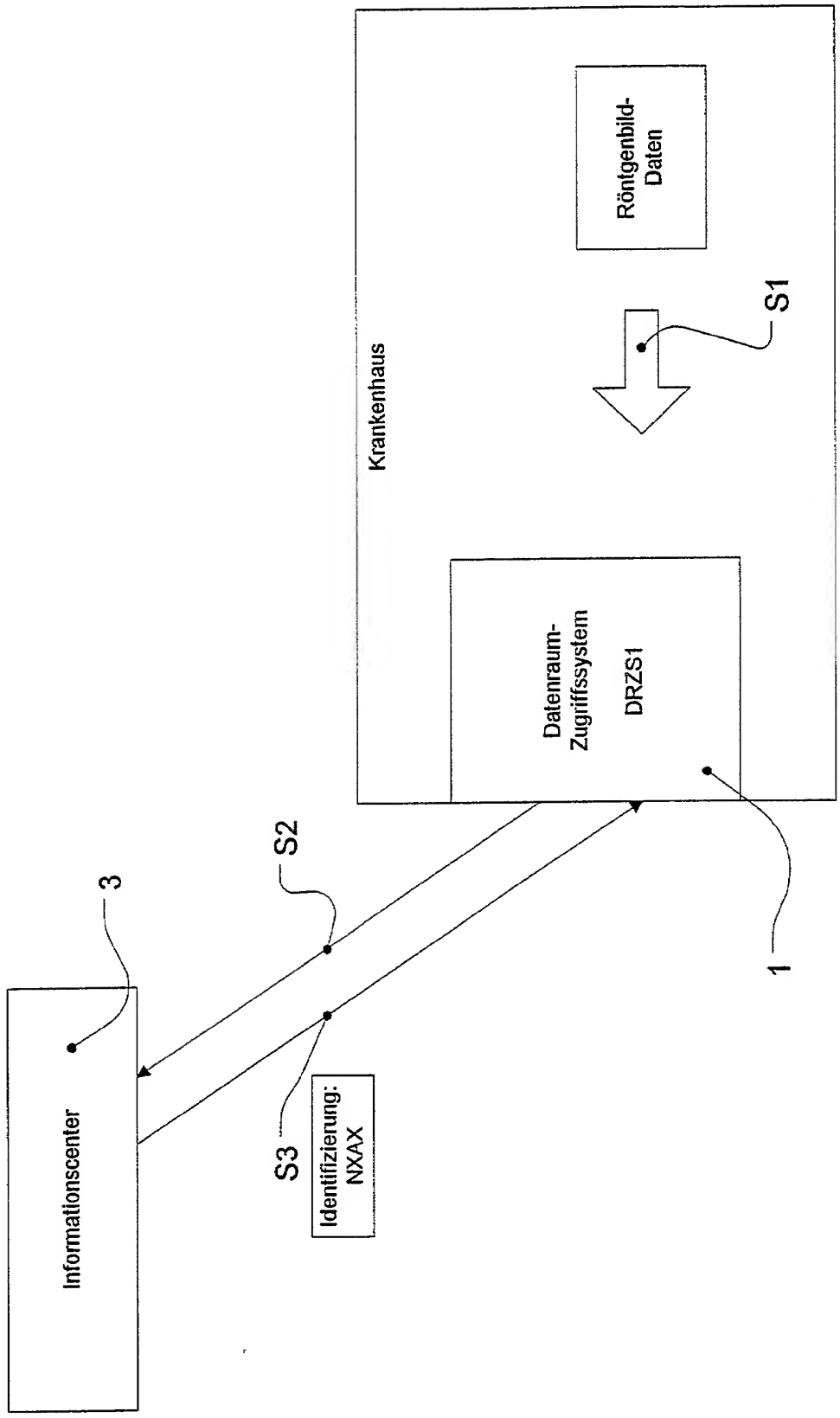
Nummer: DE 198 24 787 A1
Int. Cl.[6]: H 04 L 9/30
Offenlegungstag: 16. Dezember 1999

Fig. 1



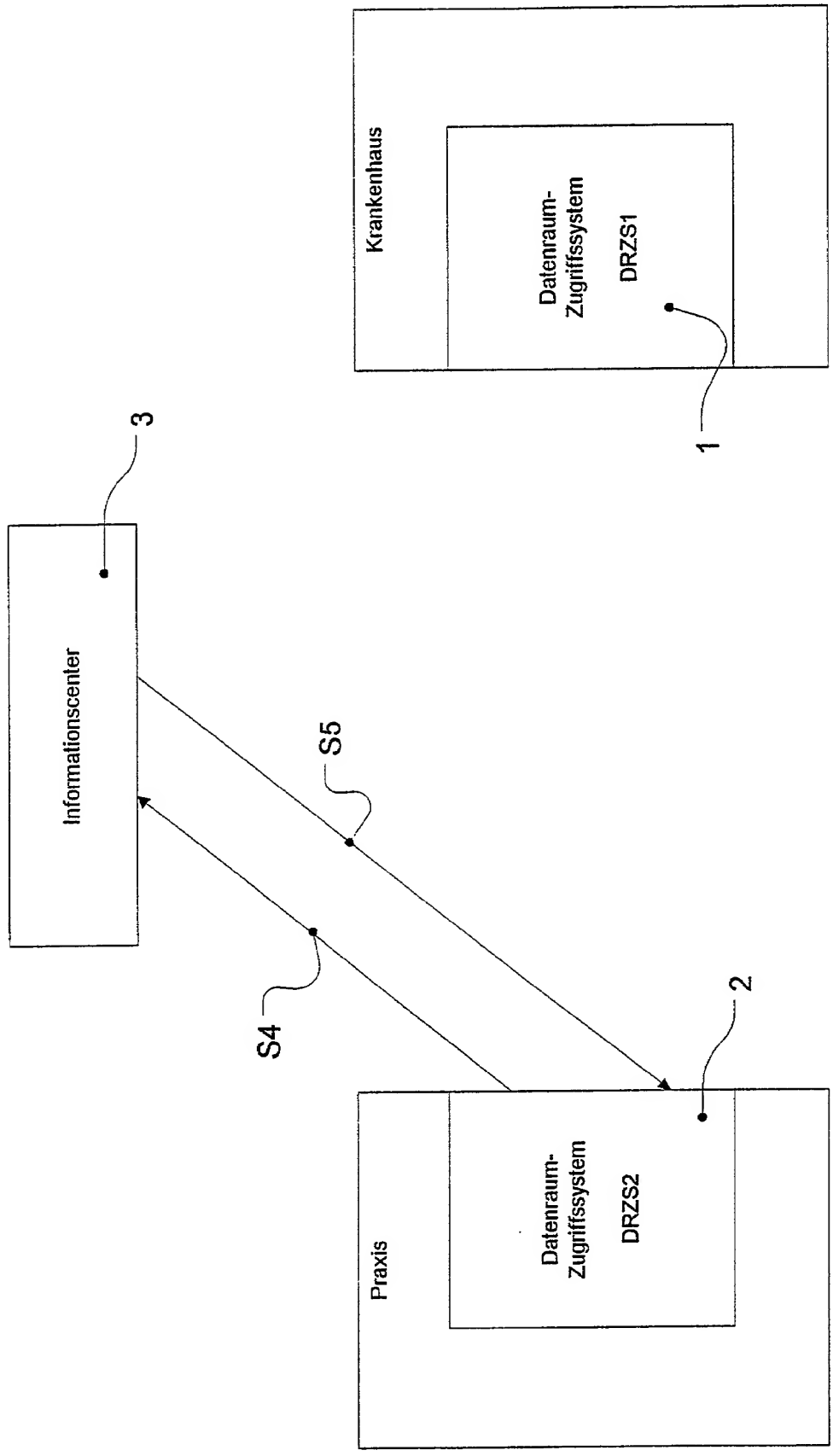
Nummer: DE 198 24 787 A1
Int. Cl.[6]: H 04 L 9/30
Offenlegungstag: 16. Dezember 1999

Fig. 2



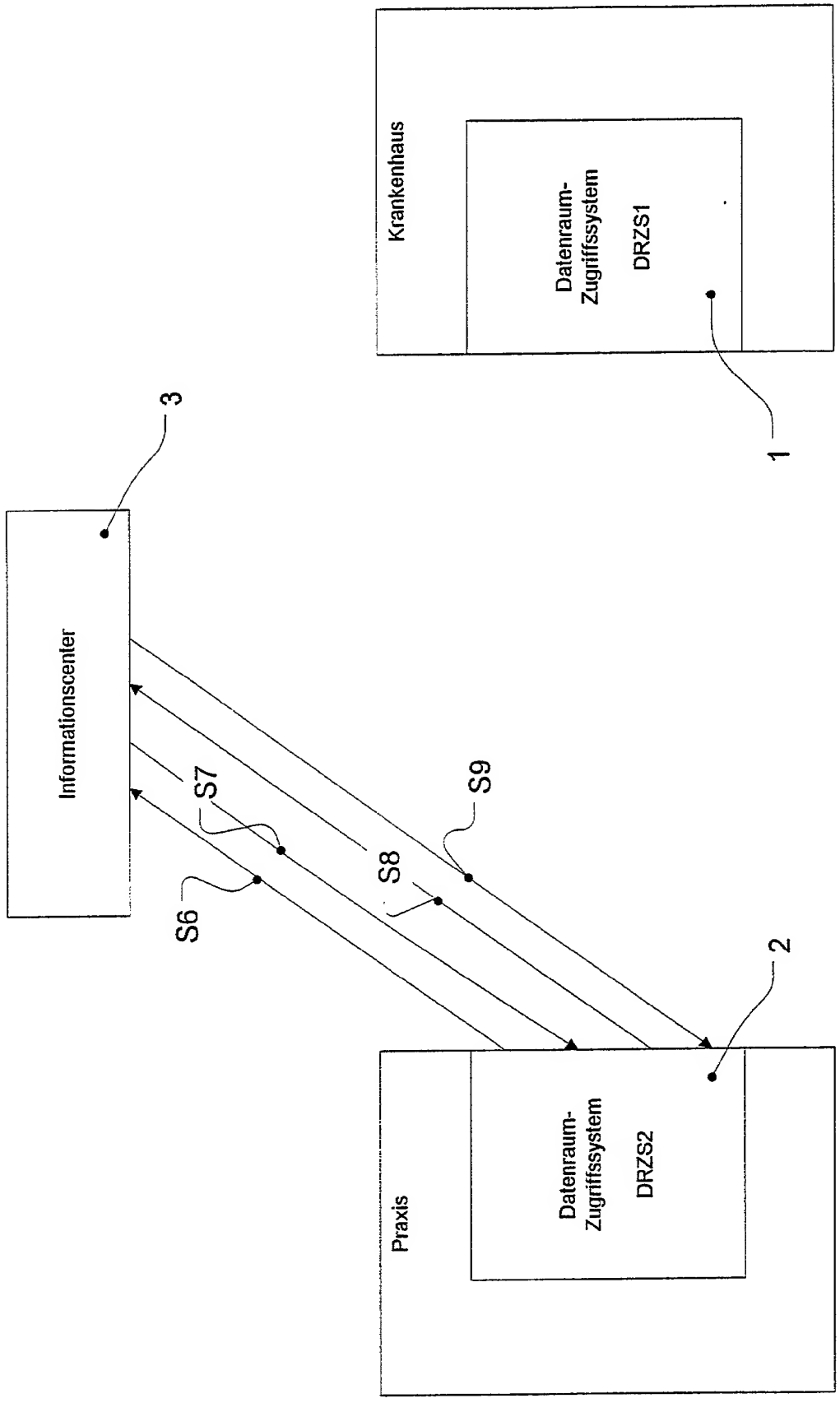
Nummer: DE 198 24 787 A1
Int. Cl.[6]: H 04 L 9/30
Offenlegungstag: 16. Dezember 1999

Fig. 3



Nummer: DE 198 24 787 A1
Int. Cl.[6]: H 04 L 9/30
Offenlegungstag: 16. Dezember 1999

Fig. 4



Nummer: DE 198 24 787 A1
Int. Cl.[6]: H 04 L 9/30
Offenlegungstag: 16. Dezember 1999

Fig. 5